ATTACHMENT 1

Selective Service System
Readiness Simulation (RS)
PERFORMANCE WORK STATEMENT (PWS)
July 22, 2026

SELECTIVE SERVICE SYSTEM (SSS)
1501 Wilson Blvd
Arlington, VA 22209

Contents

1.0 AGENCY 2

1.1 Background 2

1.2 Task Order Strategy 2

2.0 SCOPE 2

2.2 Scenario Modeling and Analytics Requirements 3

3.0 TECHNICAL REQUIREMENTS 4

4.0 DISCOVERY AND REQUIREMENTS VALIDATION 5

5.0 DELIVERABLES 6

5.1 Program Management and Administrative Deliverables 6

5.2 Technical Deliverables 6

5.3 Functional Capability Deliverables 7

5.4 Deliverable Review and Acceptance 8

6.0 PERFORMANCE STANDARDS 8

7.0 QUALITY ASSURANCE SURVEILLANCE 8

8.0 GOVERNMENT-FURNISHED INFORMATION (GFI) 8

9.0 PERIOD AND PLACE OF PERFORMANCE 9

1.0 AGENCY

The Selective Service System (SSS), established under the Military Selective Service Act (MSSA), 50 USC 3801 et seq., is responsible for maintaining a system that can rapidly furnish manpower to the Department of Defense during national emergencies while ensuring fairness, justice, and operational readiness. SSS executes its statutory mission through six Mission Essential Functions (MEFs): Registration, Selection, Notification, Delivery, Classification, and the Alternative Service Program (ASP).

This PWS defines the requirements for delivering government owned Readiness Simulation (RS) that models SSS end-to-end mobilization processes with configurable scenarios, resource constraints, and decision-support analytics.

1.1 Background

SSS currently relies on manual analysis, legacy modeling approaches, outdated assumptions, and historical datasets that do not fully reflect modern demographics, communications channels, throughput constraints, or operational readiness conditions. A unified simulation environment is necessary to:

- Evaluate staffing and resource requirements
- Compare mobilization and policy scenarios
- Assess the operational impact of surge conditions
- Identify throughput risks, delays, and bottlenecks
- Support executive planning and reporting obligations

The RS must be hosted within SSS-designated information technology (IT) environments, operate on anonymized aggregate data, and comply with FISMA Moderate and Agency security requirements.

1.2 Task Order Strategy

The Government intends to issue a contract under this PWS for the development, configuration, integration, delivery, training, and transition of the RS. Requests may be structured as:

- Discovery and Requirements Validation efforts to refine assumptions, workflows, and data needs
- Design and Implementation efforts to build and integrate the RS engine, scenario manager, and reporting capabilities
- Documentation and Knowledge Transfer efforts to ensure long-term government sustainment
- Security and Compliance activities supporting Interim Authority to Test (IATT) and Authority to Operate (ATO) readiness

Subsequent in scope requests via modifications may support enhancements, scenario expansions, maintenance, or additional analytical modules.

2.0 SCOPE

The Contractor shall design, develop, validate, document, and deliver a government owned RS that models the full end-to-end SSS mobilization pipeline, supports configurable scenarios, and provides decision-support analytics

necessary for leadership, planners, and operators. The RS shall operate within an SSS-designated cloud environment, use anonymized aggregate data, and support complete Government ownership and sustainment.

2.1 Model Architecture and MEF Coverage

- Implement a discrete event simulation (DES) based representation of Registration, Selection, Notification, Delivery, Classification, and ASP
- Model queues, routing, service times, and resource constraints
- Support timing windows
- Represent MEPS throughput, no-shows, medical disqualification rates, claims processing, and ASP diversion
- Support surge, degraded operations, policy toggles, and stochastic behavior

2.2 Data, Scenario Modeling, and Analytics Requirements

The Contractor shall:

- Identify, validate, and supply required data inputs, parameter sets, modeling assumptions, and industry benchmarks — recognizing that legacy SSS draft data may be outdated or unreliable
- Document all data sources, benchmark methodologies, and parameter derivations to ensure transparency, repeatability, and defensibility of analytical outputs
- Provide baseline, surge, degraded operations, and policy scenarios
- Generate staffing requirement outputs by office
- Provide parameter files and assumption transparency
- Support user-modifiable inputs and parameters
- Provide Monte Carlo uncertainty analysis and sensitivity analysis
- Provide for scenario comparisons
- Support dashboards and reports compatible with Excel, Power BI, CSV, and PDF
- Support after-action reconstruction for historical or exercise-driven inputs

2.3 Security, Compliance, and Risk Management

- Comply with FISMA Moderate, NIST SP 800-53, FIPS 140-3, EO 14028
- Support Microsoft Entra ID (SAML 2.0) authentication
- Provide Software Bill of Material (SBOM)
- Support OMB M-21-31 audit logging
- Provide SAST/DAST reports

- Provide source code, build pipelines, Infrastructure as Code (IaC), and configuration files
- Support secure deployment, rollback, and operations

Use of COTS Tools:

If the Contractor proposes the use of Commercial Off the Shelf (COTS) DES software or other proprietary components, the Contractor shall identify all associated licensing requirements, runtime dependencies, and any recurring costs. The Government shall not incur any licensing fees, subscriptions, or renewal costs unless such costs are explicitly disclosed, priced, and approved as part of the awarded contract

---

3.0 TECHNICAL REQUIREMENTS

The Contractor shall provide secure, scalable, maintainable, interoperable, and cloud-capable enterprise solutions that support current and future SSS operational requirements.

The RS shall:

- Operate at daily timestep granularity (per-registrant microsimulation is out of scope)
- Ingest and use anonymized aggregate data only
- Incorporate logic that maps workload and MEF responsibilities to specific SSS offices and Directorates, enabling the system to estimate office-level staffing demands required to execute mobilization tasks
- Comply with FISMA Moderate, NIST SP 800-53, OMB M-21-31 audit logging, FIPS 140-3, EO 14028 requirements, and Section 508 accessibility
- Support Microsoft Entra ID authentication using SAML 2.0. Administrative or Privileged access will enforce MFA
- Provide full source code, build pipelines, schema definitions, Infrastructure-as-Code Terraform artifacts, and configuration files
- Support deployment, rollback, and test automation via provided documentation
- Include SAST/DAST security testing with results provided to SSS
- Include mechanisms for ingesting Contractor-provided updated data, validated parameter files, and benchmark references

The Contractor shall ensure compliance with all applicable Federal laws, regulations, standards, policies, and guidance in effect at the time of contract award and throughout contract performance, including but not limited to:

- Federal Information Security Modernization Act (FISMA)
- NIST SP 800-53, NIST SP 800-63 and other applicable NIST guidance
- Federal Risk and Authorization Management Program (FedRAMP), where applicable
- Section 508 of the Rehabilitation Act
- Federal Records Act and National Archives and Records Administration (NARA) requirements

- All applicable Federal records management laws, regulations, policies, and procedures, including those issued by NARA
- Applicable Office of Management and Budget (OMB) memoranda
- Applicable Binding Operational Directives (BODs) or Emergency Directives (EDs)
- Applicable Executive Orders (EOs) governing cybersecurity, digital modernization, records management, and Federal information systems

3.1 COTS LICENSING REQUIREMENTS

If the RS is developed using COTS DES software or other proprietary tools, the Contractor shall:

- Solicit approval from the Government to use any recommended tools;
- Provide a complete description of the licensing model (e.g., perpetual, annual subscription, per seat, server based, or runtime)
- Identify all licenses required for Government operation, including developer, runtime, analytics, or server components
- Ensure that all license costs required for development, testing, deployment, sustainment, or Government operation are separately priced
- Ensure that the Government can operate, modify, and sustain the RS without requiring contractor-exclusive development licenses
- Ensure that the RS remains functional and accessible without degradation if licenses are not renewed, unless such renewal is expressly required and approved by the Government

---

4.0 DISCOVERY AND REQUIREMENTS VALIDATION

The Contractor shall conduct a Discovery Phase to validate operational workflows and MEF processes; identify data sources and parameters; define the analytical approach for generating staffing requirements by office; conduct SME workshops; map assumptions, dependencies, and constraints; and produce a Conceptual Model and Implementation Plan.

At the conclusion of the Discovery Phase, the Contractor shall provide, at a minimum:

- Discovery Report
- Validated Requirements
- Conceptual Model
- Assumptions Register
- Comprehensive Data and Benchmark Justification Package
- Preliminary Implementation Plan

The Contractor shall not begin implementation, migration, development, or configuration tasks until the Government reviews and approves the Discovery deliverables.

5.0 DELIVERABLES

The Contractor shall provide all management, administrative, technical, operational, security, training, and sustainment deliverables necessary to support successful execution of this contract.

Unless otherwise specified all deliverables shall be submitted electronically in Government-approved formats. The Government reserves the right to review, comment on, reject, or require revision of submitted deliverables that do not meet contract requirements.

Deliverables identified within this section are representative baseline requirements. Additional deliverables, milestones, acceptance criteria, and reporting requirements may be identified at the task order level.

5.1 Program Management and Administrative Deliverables

The Contractor shall provide the following program management and administrative deliverables in support of contract execution, coordination, governance, reporting, and oversight activities.

Deliverable	Description	Frequency	Format	Submit To
Project Charter	Defines scope, objectives, governance structure	Initial and updates	MS Office/PDF	COR
Communication Plan	Meetings, cadence, roles, reporting	Initial and updates	MS Office/PDF	COR
Integrated Master Schedule	Activities, milestones, dependencies	Monthly	MS Project/PDF	COR
Weekly Status Reports	Progress, risks, issues	Weekly	MS Office/PDF	COR
Monthly Program Report	Performance summary	Monthly	MS Office/PDF	COR
Quarterly Review Briefing	Executive readiness review	Quarterly	PPT/PDF	COR & Stakeholders
Risk Register	Technical/operational/cyber risks	Monthly	MS Office/PDF	COR
Staffing Plan	Personnel, roles, onboarding	Initial and updates	MS Office/PDF	COR

5.2 Technical Deliverables

The Contractor shall provide technical, engineering, operational, cybersecurity, testing, deployment, and sustainment documentation necessary to support implementation, operation, maintenance, authorization, and transition activities.

Deliverable	Description	Frequency	Format	Submit To
System Architecture Documentation	Logical/physical/integration architecture	Initial + updates	MS Office/Visio/PDF	COR
Data & Benchmark Validation Package	Contractor-provided datasets, parameters, benchmark references, and methodology documentation	Initial + updates	MS Office /PDF	COR

Data Mapping/Migration Docs	Mapping, transformations, validations	Per cycle	MS Office /PDF	COR
Security Documentation	SBOM, SAST/DAST, audit logging, ATO/SSP artifacts for shared controls	As required	MS Office /PDF	COR/ISSO
Test Plans & Results	Test cases and validation	Per phase	MS Office /PDF / SSS-Maintained GitHub Repository	COR
Deployment & Rollback Procedures	Deployment artifacts	Pre-production	MS Office /PDF	COR
Runbooks	Operations procedures	Pre-handoff	MS Office /PDF	COR
Licensing and Runtime Dependency Documentation	Provides a complete Bill of Materials (BOM) for all licensing requirements and runtime dependencies	Initial + updates	MS Office / PDF	COR
Application Source Code	All source code, including build files, necessary to build the entire RS.	Per commit	SSS-maintained GitHub repository	COR
Infrastructure-as-Code	All configuration files necessary to define the entire Cloud environment including build pipelines.	Per commit	SSS-maintained GitHub repository	COR

5.3 Functional Capability Deliverables

The Contractor shall deliver a government-owned, stand-alone RS and associated functional capabilities required for initial development, configuration, integration, and delivery. This contract covers design and delivery activities only. Ongoing operation, maintenance, or sustainment of the RS is not within the scope of this PWS unless explicitly identified in a future task order.

Capability delivery requirements shall be defined at the task order level and may include, but are not limited to, the following functional capability areas:

Deliverable	**Description**
Fully Functional DES Model	End-to-end RS model covering all MEFs
Scenario Library	Baseline, surge, degraded, policy scenarios
Dashboard Suite	KPIs, analytics, visualizations
Monte Carlo & Sensitivity Modules	Uncertainty and scenario analysis
Export Tooling	Excel, CSV, PDF, Power BI
Documentation Suite	Operator/Admin/Developer guides
Training & Knowledge Transfer	Training sessions for SSS staff

Specific implementation milestones, operational acceptance criteria, deployment schedules, testing requirements, security requirements, and transition requirements shall be identified at the task order level.

5.4 Deliverable Review and Acceptance

The Government will review submitted deliverables for completeness, accuracy, quality, compliance, and alignment with contract requirements.

The Contractor shall correct identified deficiencies and resubmit deliverables within timelines specified by the Government.

Government review or acceptance of deliverables shall not relieve the Contractor of responsibility for meeting contract requirements, performance standards, security requirements, or operational objectives.

6.0 PERFORMANCE STANDARDS

The Contractor shall meet the following minimum performance standards unless otherwise specified at the task order level:

Performance Area	Standard
System Availability	99.9% uptime during operational periods
Vulnerability Remediation	Within BOD 26-4 defined timelines
Incident Response Acknowledgement	Within 1 hour
Data Backup Validation	Quarterly
Deliverable Timeliness	95% on-time delivery
User Access Provisioning	Within 1 business day of approval
Defect Resolution for Critical Issues	Within 24 hours

7.0 QUALITY ASSURANCE SURVEILLANCE

The Government will monitor Contractor performance through review of deliverables, status reports, system metrics, testing activities, security assessments, operational demonstrations, and other surveillance methods as determined appropriate by the Government.

The Contractor shall support performance monitoring, quality assurance reviews, operational testing, inspections, and corrective action activities throughout the period of performance.

8.0 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide:

- Access to SSS-designated cloud development environments

- Relevant operational data, documentation, policies, and SME support
- Access to applicable SSS systems, facilities, and GFE

The Contractor shall ensure appropriate handling, safeguarding, and use of all GFI.

9.0 PERIOD AND PLACE OF PERFORMANCE

The period of performance shall be defined at the task order level. The anticipated duration for initial delivery is **6–12 months**, depending on validated requirements. Work may be performed at Government facilities, Contractor facilities, or approved remote locations.